REMARKS

Applicant respectfully requests reconsideration and allowance of the subject application in view of the foregoing amendments and the following remarks.

Claims 1, 3-4, 7-14, 31-34, 37-38, 40-41 and 44-46 are pending in the application, with claims 1, 31, and 40 being independent. Claims 2, 39 and 50-53 were previously canceled. Claims 1, 31-34, 38, 40, and 46 are amended herein. Support for the claim amendments and additions can be found in the original disclosure. No new matter has been added.

STATEMENT OF SUBSTANCE OF INTERVIEW

Initially, Applicant wishes to thank the Examiner for conducting an interview with Applicant's representatives, Elliott Chen along with Elizabeth Zehr, on Wednesday February 11, 2009.

During the interview, Applicant's representatives and the Examiner discussed the §112 and §103(a) rejection as applied to claim 1. Specifically, the Examiner proposed additional amendments to Applicant's proposed amendments in order to clarify the elements that Applicant argues are distinguishable from the cited art. Applicant's attorney understood the Examiner to agree that incorporating the proposed amendments into the independent claims overcomes at least the cited art; however, an expanded search would be conducted. Applicant thanks the Examiner for this indication and has presented presently pending independent claims 1, 31, and 40 accordingly.

The subject matter of the interview, and other remarks, are included below under their respective sections to assist the Examiner in more fully understanding the Applicant's position on the rejections under §103(a).

§ 112, FIRST PARAGRAPH REJECTIONS

The Office rejected claims 1, 3-4, 7-14, and 41 under 35 U.S.C. §112, first paragraph as failing to comply with the written description requirement. This rejection is respectfully traversed.

Specifically, the Office maintains:

> The amended claim 1 recites the limitations "returning a fail value when each of the plurality of security engines has determined that it is not ready to begin using the new security policy; returning a pass value when each of the plurality of security engines has determined that it is ready to begin using the new security policy" (lines 9-12). Whereas the disclosure describes that each security engines returns either a failure or an OK value depending on whether the security engine itself has successfully processed the new policy, the disclosure does not describe returning the OK/ failure value when each of the security engines has successfully/unsuccessfully processed the new policy. Therefore, the limitations are considered new matter. Claims 41 is rejected on the same basis as claim 1.

(Office Action, Page 3). Applicant has herein amended claims 1 and to cure the written description rejection cited by the office. Specifically, claim 1 has been amended to recited "returning, via each of the plurality of security engines, a fail value when it determines that it has not successfully processed the identified set of rules." Additionally, claim 41 has been amended to remove the reference to "returning a fail value when each of the plurality of security engines has determined that it is not ready to begin using the new security policy; returning a pass value when each of the plurality of

security engines has determined that it is ready to begin using the new security policy." Claims 3-4, and 7-14 depend from independent claim 1. Applicant submits that claims 1, 3-4, 7-14, and 41, as amended, comply with the requirement of 35 U.S.C. §112, first paragraph.

In accordance with the above, the Applicant respectfully requests reconsideration and withdrawal of the rejection to claims 1, 3-4, 7-14, and 41 under 35 U.S.C. § 112, first paragraph.

§ 103 REJECTIONS

Claims 1, 3-4, and 7-14 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent Publication No. 2005/0044418 ("Milliefsky") in view of 2004/0003266 ("Moshir") and further in view of "An Introduction to Database System" ("Date"). Claims 31-34, 37-38, 40-41, and 44-46 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Moshir in view of Date. Applicant respectfully traverses the rejection, and requests that the rejection be reconsidered and withdrawn.

Miliefsky is directed to "a proactive network security system to protect against hackers for the proactive automated defense against hackers by automatically finding, reporting, communicating with countermeasures about and removing the common vulnerabilities and exposures (CVEs) that they exploit." (Paragraph [0012]). More specifically, a "dynamic updates engine securely communicates with and authenticates to a remote updating service." (Paragraph [0041]). The communication between the dynamic updates engine and the remote updating service includes "requesting authentication and access to the updating service, requesting updates from the updating

service, informing the updating service about system health and other non-privacy related system features and issues which may enable enhancements to the quality and proactive nature of the Anti-Hacker System." (Id.).

Moshir generally pertains to discovering software updates, discovering if a given computer can use the software update, and then updating the computers with software as needed automatically across a network without storing the updates on an intermediate machine within the network. (Summary). In addition, Moshir pertains to detecting failures, stopping a rollout, and removing software from computers that were already updated. (Id.).

Independent claim 1, as presently presented, recites:

> A method, implemented in a computing device, the method comprising:
>
> accessing a new security policy to be implemented by a plurality of security engines of the computing device and to be implemented by the plurality of security engines in place of a current security policy, the new security policy including a first set of rules specific to a first type of security engine and a second set of rules specific to a second type of security engine;
>
> identifying, by a rule set generator of the computing device, which set of rules is used by which type of security engines;
>
> processing, via each of the plurality of security engines, the identified set of rules specific to its type to establish new rules for operation of the security engine while the security engine continues to operate according to previous rules;
>
> returning, via each of the plurality of security engines, a fail value when it determines that it has not successfully processed the identified set of rules;
>
> returning, via each of the plurality of security engines, a pass value when it determines that it has successfully processed the identified set of rules;
>
> receiving an indication to ignore the new rules and continue operating each of the plurality of security engines according to the

previous rules when at least one of the plurality of security engines has returned a fail value; and

switching, after receiving a pass value from each of the plurality of security engines, each of the plurality of security engines to the new rules substantially concurrently.

Applicant respectfully submits that Miliefsky, Moshir and Date whether taken alone or in combination, fail to teach or suggest the recitations of claim 1 for at least two reasons. First, Miliefsky in view of Moshir and Date fails to teach or suggest "the new security policy including a first set of rules specific to a first type of security engine and a second set of rules specific to a second type of security engine."

The Office cites paragraph [0041] of Miliefsky as teaching the security policy of claim 1. Applicant provides the relevant sections of Miliefsky that was cited by the Office:

> The dynamic updates engine securely communicates with and authenticates to a remote updating service which may be hosted through a virtual private network or through a strong-encrypted web-based service running on a system which is publicly assessable through an IP Address and an HTTPS or other SSL-based connection. The Dynamic Updates Engine functions include requesting authentication and access to the updating service, requesting updates from the updating service, informing the updating service about system health and other non-privacy related system features and issues which may enable enhancements to the quality and proactive nature of the Anti-Hacker System.

(Paragraph [0041]). Although Miliefsky teaches a Dynamic Updates Engine that requests updates from an updating service, there is nothing in Miliefsky to suggest that the updates comprise multiple sets of rules to be implemented on multiple types of security engines as recited in claim 1. Additionally, Moshir fails to remedy the deficiencies of Miliefsky noted above with respect to claim 1.

Moshir teaches updating a target computer with "any of a wide variety of software that can be updated across a network, such as an incremental software patch, a new software program never before installed on the target computer, an update to an old program, software scripts, data files, or even an update of the update agent." (Paragraph [0069]). This update software can either be downloaded to a single target computer (paragraph [0072[) or it can be downloaded to multiple target computers (paragraph [0075]).

Regardless of whether the software of Moshir is being used to update a single computer or multiple target computers, Applicant submits that the entire software update is downloaded to the target computer(s). Since Moshir teaches updating every target computer with the same piece of software, Moshir fails to teach or suggest a security policy that includes "a first set of rules specific to a first type of security engine and a second set of rules specific to a second type of security engine" as recited in claim 1. Date was not cited for the security policy and thus Date fails to remedy the deficiencies in Miliefsky and Moshir noted above with respect to claim 1.

Second, Miliefsky in view of Moshir and Date fails to teach or suggest "identifying, by a rule set generator of the computing device, which set of rules is used by which type of security engines." As provided in the remarks above, Applicant submits that Moshir teaches downloading the same piece of software to one or more target computers. Since the same piece of software is being downloaded to the target computer, Moshir fails to teach or suggest identifying "which set of rules is used by which type of security engines"

as recited in claim 1. Neither Miliefsky nor Date remedy this deficiency with respect to claim 1.

Due to the Applicant's earnest belief that the claim 1, as rejected under Section 103(a), is allowable for reciting elements which are not taught or suggested in the cited references, Applicant will not address motivation to combine with respect to claim 1 during this response. However, Applicant hereby reserves the right to further challenge motivation to combine the cited references.

The amendments to claim 1 are supported by the specification on at least page 7, lines 1-16 and on page 8, lines 1-14. No new matter is added. Accordingly, independent claim 1 is believed allowable.

Dependent claims 3-4, and 7-14 depend from independent claim 1 and are allowable by virtue of this dependency, as well as for additional features that they recite. Applicant also respectfully requests individual consideration of each dependent claim.

Accordingly, claims 3-4, and 7-14 are allowable for at least the foregoing reasons.

Independent claim 31, as presently presented, recites:

> One or more computer readable storage media storing one or more instructions that, when executed by one or more processors, causes the one or more processors to:
>
> receive information of a new security policy to be used by a plurality of security engines, the new security policy including a first set of rules specific to a first type of security engine and a second set of rules specific to a second type of security engine;
>
> *identify, by a rule set generator of the computer readable storage media, which set of rules is used by which type of security engines;*

process, via each of the plurality of security engines, the identified set of rules specific to its type to generate new rules having associated data for operation of the security engine;

use a previous set of rules and associated data when each of the plurality of security engines determines that it has not successfully processed the identified set of rules; and

use, upon receiving an indication that each of the plurality of security engines determines that it has successfully processed the identified set of rules, the new set of rules and associated data.

(Emphasis added). Applicant respectfully submits that Moshir and Date whether taken alone or in combination, fail to teach or suggest the recitations of claim 31. Specifically, as discussed during the Examiner Interview, Moshir in view of Date fails to teach or suggest enforce "identifying, by a rule set generator of the computer readable storage media, *which set of rules is used by which type of security engines*" as recited in claim 31. (Emphasis added).

The Office acknowledges that, with reference to the rejection of claim 31: "Moshir discloses . . . each of the security engines returning a pass value when the security engine has determined that it is ready to begin using the new security policy (i.e., update installs properly) . . . (paragraphs 0074-0078)." (Office Action, page 6). Applicant submits that paragraphs 0074-0078 of Moshir teach installing the entire contents of the update material on all of the target computers. Applicant's claim 31, on the other hand, identifies "which set of rules is used by which type of security engines" and thus is not anticipated by Moshir.

Furthermore, Date fails to remedy the deficiencies in Moshir noted above with respect to claim 31.

The amendments to claim 31 are supported by the specification on at least page 7, lines 22-25. No new matter is added. Accordingly, independent claim 31 is believed allowable.

Dependent claims 32-34, and 37-38 depend from independent claim 31 and are allowable by virtue of this dependency, as well as for additional features that they recite. Applicant also respectfully requests individual consideration of each dependent claim.

Accordingly, claims 32-34, and 37-38 are allowable for at least the foregoing reasons.

Independent claim 40, as presently presented, recites:

> A method, implemented in a security engine of a computing device, the method comprising:
>
> receiving a new security policy to be enforced by a plurality of security engines of the computing device, the new security policy including a first set of rules specific to a first type of security engine and a second set of rules specific to a second type of security engine;
>
> identifying, by a rule set generator of the computing device, which set of rules is used by which type of security engines;
>
> processing, via each of the plurality of security engines, the identified set of rules specific to its type to establish new rules for operation of the security engine while the security engine continues to operate according to previous rules; and
>
> enforcing, in response to receipt of an indication that each of the plurality of security engines has determined that it has successfully processed the identified set of rules, the new rules on each of the plurality of security engines.

Applicant respectfully submits that Moshir and Date whether taken alone or in combination, fail to teach or suggest the recitations of claim 40. Specifically, as discussed during the Examiner Interview, Moshir in view of Date fails to teach or suggest

"identifying, by a rule set generator of the computing device, which set of rules is used by which type of security engines" as recited in claim 40.

Accordingly, independent claim 40 is believed allowable.

Dependent claims 41, and 44-46 depend from independent claim 40 and are allowable by virtue of this dependency, as well as for additional features that they recite. Applicant also respectfully requests individual consideration of each dependent claim.

Accordingly, claims 41, and 44-46 are allowable for at least the foregoing reasons.

CONCLUSION

For at least the foregoing reasons, it is respectfully submitted that claims 1, 3-4, 7-14, 31-34, 37-38, 40-41 and 44-46 are in condition for allowance. Applicant respectfully requests reconsideration and withdrawal of the rejections and an early notice of allowance.

The arguments and amendments presented herein were necessitated by the most recent Office Action, and could not have been presented previously because Applicant earnestly believed that the claims were in condition for allowance at the time of filing the previous response.

If any issue remains unresolved that would prevent allowance of this case, **Applicant requests that the Examiner contact the undersigned attorney to resolve the issue.**

Respectfully Submitted,

Lee & Hayes, PLLC

Dated: March 18, 2009 By: _____

Damon J. Kruger
Reg No. 60400
Elizabeth J. Zehr
Reg No. 64013
Lee & Hayes, PLLC
206-315-4001